



## **Aus der Praxis: Mobile Geräte sicher einsetzen**

- | Thomas Zysk
- | Account Manager



| Vorstellung Acteos

| Praxisbezogenen Verwendung mobiler Endgeräte

| Risiken und Gefahrenpotentiale

| Sicherheit



## Acteos GmbH & Co. KG

| Integration von mobilen Lösungen (Hard- und Software)

| In Unternehmenskritischen Bereichen

| Für den Mittelstand und Großunternehmen

| Alles aus einer Hand





## Anwendungsbereiche

| Field Service ➔ **Logonsite Plus**

| Warehouse, Transportlogistik ➔ **Logeye**

| Mobile Sales ➔ **Loginspect**

| Kundenspezifische Lösungen



| Sicherheitsaspekte bei der Verwendung von mobilen Endgeräten |

| Sicherheitsrisiken durch externe Gefahren

| Sicherheitsrisiken durch interne Gefahren



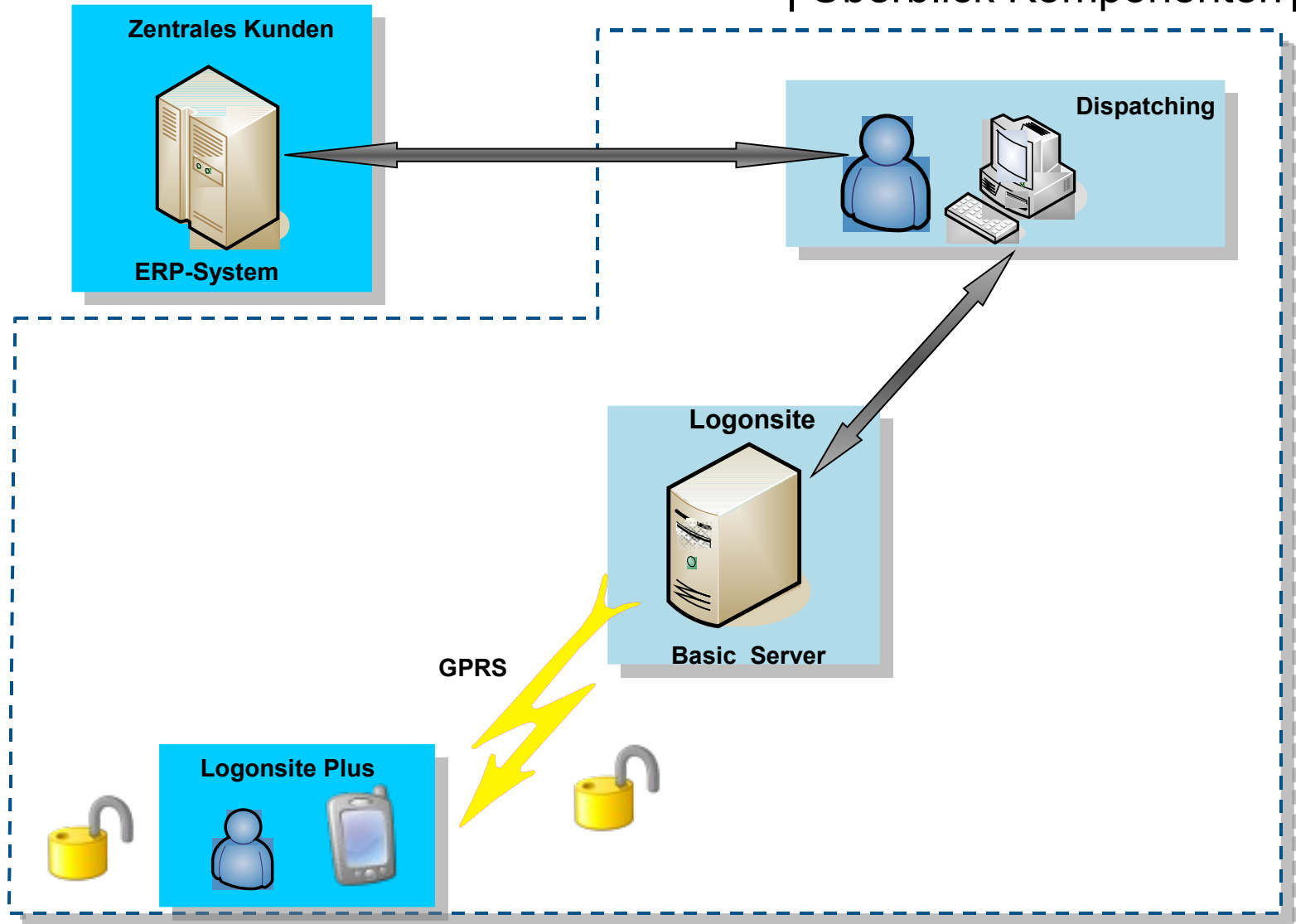
| Überblick Logonsite Plus

| Komponenten

| Sicherheit



| Überblick Komponenten |



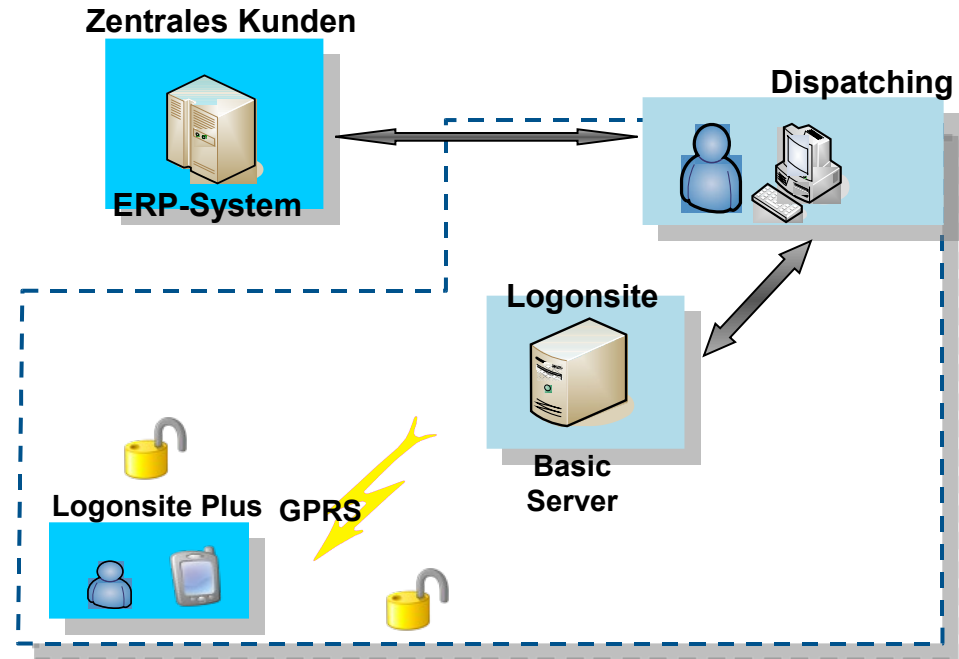
| Überblick Logonsite Plus

| Komponenten

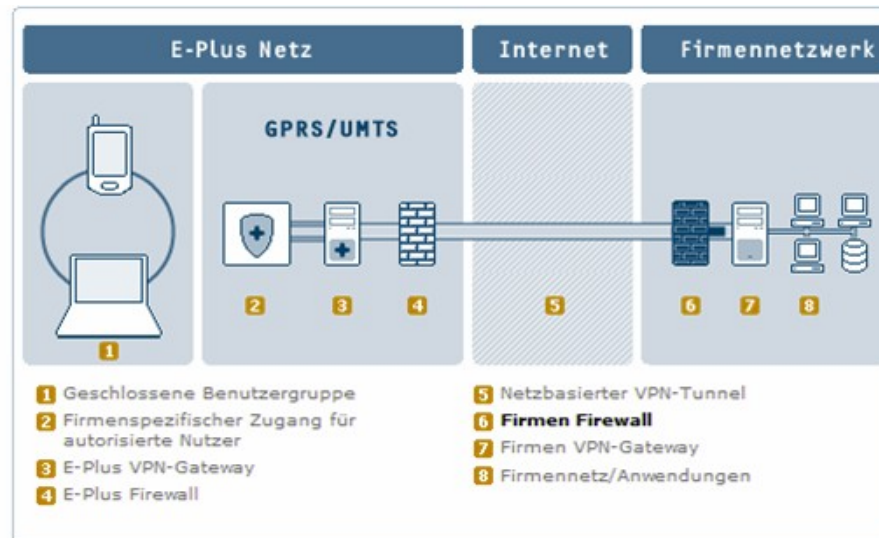
| Funktionen



- IP VPN
- Gerätesperrung
- Ablaufüberwachung
- Gerätesteuerung
- Kontaktlose Geräte



### | Online IP-VPN



Einrichtung einer geschlossenen Benutzergruppe.

Nur registrierte SIM Karten werden zur Anmeldung am Server zugelassen.

Datenaustausch über einen gesicherten VPN-Tunnel.



**PDA'S,  
Windows Mobile**



**Tablet-PC oder  
Notebooks,  
Windows XP, Vista**



## | Erweiterte Sicherheit



### Advanced Security

#### **Gerätesperrung:**

Einrichtung eines Standard-Screens und der Windows-Starttaste durch einen - auf Kundenwünsche anpassbaren - Home-Screen.

Dadurch lediglich Zugriff auf bestimmte Anwendungen und Webseiten erlaubt. Kein Zugriff auf die Gerätesteuerung möglich.

Das verringert die Höhe, der durch veränderte Benutzereinstellungen verursachten Ausfallzeiten.



## | Erweiterte Sicherheit



### Advanced Security

#### **Ablaufüberwachungsverfahren für Anwendungen:**

Direkt in das Betriebssystem integrierte Security, um zu verhindern, dass zugangsbeschränkte Anwendungen auf mobilen Geräten laufen.

Daher keine „Fremdsoftware“ lauffähig.

Hohe Effizienz gegenüber den üblichen Black- oder Whitelist-Lösungen, da keine erhöhte Akkubelastung oder CPU-Nutzung.



## | Erweiterte Sicherheit



### Advanced Security

#### **Steuerungsverfahren der Gerätefunktionen:**

Spezielle Steuerungsverfahren erlauben die Hardwarefunktionen der Geräte selektiv zu deaktivieren.

Erstellung individueller Profile für verschiedene Benutzer oder Niederlassungen innerhalb eines Unternehmens.

Gezielte Deaktivierung der Bluetooth- und Infrarot-Anschlüsse ist genauso möglich wie das Abschalten von Kameras und anderen Hardwarefunktionen wie USB oder Bluetooth-Schnittstellen.

Daher kein unerlaubter Download von Daten durch eigene Mitarbeiter.



## | Erweiterte Sicherheit



### Advanced Security

#### **Verfahren kontaktloser Geräte:**

Verwaltet die Sicherheit auf “kontaktlosen” Geräten, die nicht in der Lage sind sich mit der Zentrale zu verbinden.

Geräte werden z.B. offline geschaltet, wenn innerhalb eines bestimmten Zeitintervalls nicht kontaktiert wurde.

Sicherheit bei Verlust oder Diebstahl.



| Fazit

Vertrauen ist gut, Kontrolle ist besser!

Es gibt nicht nur den bösen Hacker, sondern auch den b.... Mitarbeiter!

..... und

Acteos bietet praxiserprobte Lösungen um Ihre Daten zu schützen.





# **Vielen Dank für Ihre Aufmerksamkeit**

Acteos GmbH & Co. KG  
Talhofstraße 30 a  
82205 Gilching  
Germany

Tel. +49 8105 38 51-0  
Fax +49 8105-38 51-12

[www.acteos.com](http://www.acteos.com)

